



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **04358249 A**(43) Date of publication of application: **11 . 12 . 92**

(51) Int. Cl.

**G06F 13/00****G06F 15/00**(21) Application number: **03159554**(71) Applicant: **NEC CORP**(22) Date of filing: **04 . 06 . 91**(72) Inventor: **INAMI MICHIHARU**

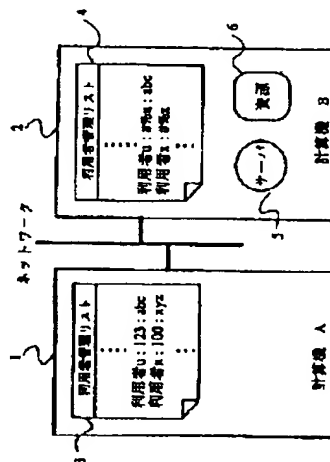
**(54) USER CERTIFYING SYSTEM FOR NETWORK  
SERVICE BETWEEN VARIOUS TYPES OF  
COMPUTER**

(57) Abstract:

**PURPOSE:** To provide the user certifying system for enabling the utilization of network service between various type computers differing the form of a user identifier used for discriminating a user.

**CONSTITUTION:** When the user of a computer A1 requests the network service through a network 1 to a server 5 on a computer B2, a local user identifier is converted to a wide area user identifier by using a user management list 3, and this identifier is transmitted to the server 5 together with the request. When a user entry coincident with the wide area user identifier in the request exists in a user management list 4, the server 5 converts the identifier to the local form user identifier of the entry.

COPYRIGHT: (C)1992,JPO&amp;Japio



(11)特許出願公開番号

(43)公開日 平成4年(1992)12月11日

### 技術表示箇所

## 【特許請求の範囲】

【請求項1】 通信ネットワークで接続された異なる利用者識別子形式を持つ異機種計算機間で、相互の計算機上の資源を共有するネットワークサービスにおける利用者認証方式において、各計算機が使用する利用者管理リストのエントリとして、利用者に対するローカル形式の利用者識別子と、計算機固有の利用者識別子形式に依存しない形式の大域利用者識別子を備え、ネットワークサービスをリモート計算機のサーバに要求する時に、利用者管理リストからローカル利用者識別子と一致するエントリに登録されている大域利用者識別子を取り出すステップと、リモート計算機への要求中に大域利用者識別子を格納してサーバへ送信するステップと、サーバにおいて、サービス要求に含まれている大域利用者識別子を利用して、リモート計算機で使用している利用者管理リストから一致する利用者エントリを検索するステップと、一致する利用者エントリが存在する場合、登録されているローカル形式の利用者識別子を与えるステップと、利用者管理リストに一致する利用者エントリが存在しない場合、特別な利用者を示すローカル形式の利用者識別子を与えるステップと、ローカル形式の利用者識別子形式を用いて資源へのアクセス権を検査するステップを含むことを特徴とする異機種計算機間ネットワークサービスにおける利用者認証方式。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 ネットワークで接続された利用者識別子の形式が異なる計算機、例えばハードウェアまたはオペレーティングシステムの種類の異なる複数の計算機が、ネットワークで接続された異機種計算機間における、ネットワークサービス利用時の利用者認証方式に関する。

## 【0002】

【従来の技術】 従来、複数の計算機をネットワークで接続したネットワークシステムにおける利用者管理は、一般に個々の計算機で行われるか、同じ利用者管理方式を用いる計算機間では論理的に集中した利用者管理が行われている。

【0003】 一般に、利用者が資源にアクセスする場合、資源が属性として持っている利用者識別子と、アクセスを要求する利用者の利用者識別子と比較してアクセス権が検査される。ネットワーク環境でも同様で、ある計算機の利用者が他の計算機の資源にアクセスする場合、一般に利用者が各計算機の利用を開始する時に認められた利用者識別子をそのまま使用して、アクセス権が検査される。

## 【0004】

【発明が解決しようとする課題】 従来のリモート資源アクセス時の利用者検査は、一般に要求側から送信される利用者識別子を使用するため、利用者識別子形式は同一

であることが要求され、異なる利用者識別子形式を用いる異なる種類の計算機システムや、異なる種類のオペレーティングシステムの計算機間では、リモート資源へのアクセスを行えないか、たとえ行えても、利用者識別子形式の異なる二種類の計算機に利用者登録を持つ同一の利用者を、ネットワークサービスにおいて同一の利用者と判断することはできない。

【0005】 本方式では上記の問題を解決した異機種計算機間ネットワークサービスにおける利用者認証方式を提供する。

## 【0006】

【課題を解決するための手段】 本方式の異機種計算機間ネットワークサービスにおける利用者認証方式は、ネットワーク上の各計算機が使用する利用者管理リストに、利用者に対するローカル形式の利用者識別子と、ローカル形式には依存しない形式の大域利用者識別子の対のエントリを備え、ネットワークサービスを利用する時に、利用者管理リストを用いてローカル形式の利用者識別子を大域識別子形式に変換するステップと、リモート計算機への要求中に大域利用者識別子を格納してサーバへ送信するステップと、サーバにおいて、転送されて来た要求に含まれる大域利用者識別子を用いて、その計算機の使用する利用者管理リストから一致する利用者エントリを検索するステップと、一致する利用者エントリが存在する場合、このエントリに登録されているローカル形式の利用者識別子を与えるステップと、一致する利用者エントリが存在しない場合、特別な利用者を示すローカル形式の利用者識別子形式を用いて資源へのアクセス権を検査するステップとを備える。

## 【0007】

【作用】 異なる利用者識別子形式を用いる計算機間でネットワークサービスを利用する場合、要求側の利用者管理リスト中の利用者のエントリから、対になっている大域利用者識別子を取り出し、その利用者識別子によりリモートに要求を行う。

【0008】 サービス提供側では、要求の一部として渡された大域利用者識別子を使用して、自身の利用者管理リストから利用者エントリを探し、一致するエントリがあればその対となって登録されているサービス提供側における利用者識別子形式に変換して資源へのアクセス権の検査に使用する。一致するエントリが存在しなければサービス提供側における特別な利用者を示す利用者識別子に変換され、資源のアクセス権の検査に使用される。

【0009】 同じ利用者識別子形式を持つ計算機間では、そのまま要求側の利用者識別子を使用することができ、種類の異なる計算機同士でアクセスを行う場合にのみ大域利用者識別子を使用してネットワークサービスにおける利用者のアクセス権を検査する。

## 【0010】

3

【実施例】本方式について図面を参照して詳細に説明する。

【0011】図1は本方式の一実施例を示す機能ブロック図である。

【0012】計算機A1と計算機B2は異なる利用者識別子の形式を持つ異なる種類の計算機で、利用者uが計算機A1の利用を開始するとき、計算機A1のシステムソフトウェアは自身の利用者管理リスト3を用いて正当な利用者であるか検査し、そうであれば利用者uに対し、利用者識別子123を与える。この利用者uはネットワークを通じて、ネットワークサーバ5を利用し、計算機B2の資源6をアクセスすることができる。また、利用者uは計算機B2が使用する利用者管理リスト4にも登録されているが、利用者管理リスト4には123のような利用者識別子形式は登録できないため、その利用者識別子は形式が異なる#σ/ouが与えられている。

【0013】利用者xは計算機A1の利用者管理リスト3には、ローカル形式の利用者識別子100と大域利用者識別子xyzが登録されているが、利用者管理リスト4にはローカル形式の利用者識別子#σ/oxしか登録されていない。

【0014】図2は異なる利用者識別子形式を持つ異種計算機間ネットワークサービスにおける利用者認証処理手順を示している。

【0015】利用者uが計算機B2のサーバ5を利用して計算機B2の資源6をアクセスする時、計算機A1では、計算機A1のシステムソフトウェアが使用する利用者管理リスト3からローカル利用者識別子123と一致するエントリを検索し、そのエントリに登録されている大域利用者識別子abcを取り出す(ステップ7)。取り出した大域利用者識別子abcを、要求と共にネットワーク通信を通じて計算機B2に送信する(ステップ8)。計算機B2上のネットワークサーバ5の機能は送信されてきた要求から大域識別子abcを取り出す(ステップ9)。計算機B2のシステムソフトウェアが使用する利用者管理リスト4から大域識別子と一致する利用者エントリを探す(ステップ10)。一致する利用者エントリが存在するので、対になって登録されている計算機B2のローカル形式の利用者識別子#%uを取り出

4

し、この利用者識別子を用いて資源へのアクセス権を検査する(ステップ11および13)。

【0016】利用者xがネットワークサーバ5を利用して計算機B2の資源6をアクセスする時、計算機A1では、計算機A1のシステムソフトウェアが使用する利用者管理リスト3からローカル利用者識別子100と一致するエントリを検索し、そのエントリに登録されている大域利用者識別子xyzを取り出す(ステップ7)。取り出した大域利用者識別子xyzを要求と共に、ネットワーク通信を通じて計算機B2に送信する(ステップ8)。計算機B2上のネットワークサービス機能を行うサーバ5は送信されてきた要求から大域識別子xyzを取り出す(ステップ9)。計算機B2のシステムソフトウェアが使用する利用者管理リスト4から大域識別子xyzと一致する利用者エントリを探す(ステップ10)。一致する利用者エントリが存在しないため、特別な利用者であることを示す利用者識別子を与え(ステップ12)、この利用者識別子を用いて資源へのアクセス権を検査する(ステップ13)。

【0017】

【発明の効果】以上説明したように、異なる利用者識別子形式を用いる計算機において、ローカルの利用者識別子の形式を変更することなくネットワーク資源に対するアクセスが行え、双方で大域利用者識別子を一致させることにより同一利用者の場合には、リモートに保有する資源に対し、所有者としてアクセスする権利があることを判断することができる。

【図面の簡単な説明】

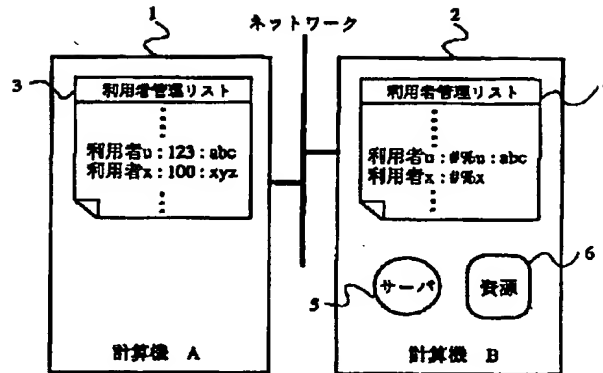
【図1】本方式の一実施例を示す機能ブロック図、

【図2】ネットワークサービスの利用者認証処理のフローチャートである。

【符号の説明】

- 1 ローカル計算機A、
- 2 リモート計算機B、
- 3 計算機Aの利用者管理リスト、
- 4 計算機Bの利用者管理リスト、
- 5 ネットワークサービスを行うサーバ、
- 6 利用者識別子を属性として持つ資源

【図1】



【図2】

